Abstract of the Invention

A method and apparatus are used to generate outputs according to a ciphering algorithm which for each of the outputs operates on a respective input using a respective key. The ciphering algorithm has a plurality of rounds in which functions are evaluated. For a least one of the functions, outputs are generated by looking up at least one look-up table with each look-up table being looked-up in parallel using respective inputs. Different methods for parallel table look-up are provided. The methods allows the ciphering algorithm to be implemented partially or entirely in parallel. An example parallel implementation involves the Kasumi algorithm in which S7 and S9 functions are evaluated in parallel for a plurality of inputs using vector instructions on an SIMD (Single Instruction Multiple Data) architecture.